AMENDMENTS TO THE SPECIFICATION

Please replace Paragraph **[0004]** with the following paragraph rewritten in amendment format:

[0004] The invention employs a portable storage device that maintains a set of one-time passwords. Using system software from a secure vantage point within the home network, the user generates a set of one-time passwords that are stored on the portable storage device. The portable storage device may then be installed in or connected to any remote client computer, giving that remote client computer the ability to establish and authenticate a secure connection with the home network. Each password is used only once, and session management software within the home network has the ability to limit a session to a predetermined length of time (e.g., 30 minutes). Although communication between home network and remote client is preferably over a secure channel, communication of the one-time password over this channel is [[is]] further protected by using an encrypted version of the user's PIN number. The PIN number is encrypted at the remote client using a plug-in module that accesses a protected area within the portable storage device to retrieve the key used for this encryption.

Please replace Paragraph **[0029]** with the following paragraph rewritten in amendment format:

[0029] The portable storage device 34 functions as a secure key distribution mechanism. The user initializes and configures the portable storage

device within the perimeter of the home network. More specifically, in the preferred embodiment the user accomplishes this using a secure interface to the portable storage device, defined within the gateway, and using secure software modules running on the gateway in a tightly controlled, secure fashion. In the preferred embodiment, the gateway includes a secure database in which the keys are also stored. This database is likewise a tightly controlled, secure entity that may be accessed only [[be]]by secure software modules running on the gateway.

Please replace Paragraph **[0031]** with the following paragraph rewritten in amendment format:

[0031] After initialization, the portable storage device may then be taken by the user to any computer anywhere in the world. By installing the portable storage device in that computer (such as in the remote client 20), the computer is rendered capable of authenticating itself for communication with the home network 22. In the presently preferred embodiment the portable storage device is provided with ~~the~~ one-time passwords during ~~the~~ initialization. Thereafter, ~~during uses~~ a plug-in program accesses ~~thesesthese~~ one-time passwords as will be more fully explained. The plug-in program may be a program module or applet suitable for use by ~~the~~ web browser software already resident on the remote client 20. The plug-in software enables the remote client 20 to participate in the exchange of messages needed for authentication. The preferred embodiment

uses the secure sockets layer (SSL) to establish a secure pipeline 38 through the internet 24.

Please replace Paragraph **[0033]** with the following paragraph rewritten in amendment format:

[0033] Once authentication has been successfully completed, the bastion host performs URL address translation and client verification services as part of the web proxy functions 48. Specifically, URLs arriving from the remote client are verified as coming from the authenticated client, and then modified specifically for that client. The web proxy system consults active state middleware (~~ASSM~~ASMM 72, Fig. 4) to determine if there is an active state for that authorized client. If so, the web proxy system accesses the trusted home network on behalf of the remote client. Notably, the address translation function is specific for each client. Re-use of URLs is prohibited, thus thwarting a system attack where URLs for an authenticated client are intercepted and reused by an impostor. Further details of this process are described below in connection with Figure 9.

Please replace Paragraph **[0035]** with the following paragraph rewritten in amendment format:

[0035] The bastion host includes a session manager that requires authentication using a one-time password. For added security, the session manager also controls the length of the session[[,]] by terminating the session

after a predetermined time (e.g., 30 minutes). These control functions are illustrated at 54. The session manager performs the authentication function by interaction with the plug-in software within the portable storage device as depicted at 56.[[.]]

Please replace Paragraph **[0048]** with the following paragraph rewritten in amendment format:

[0048] Referring to Figure 6, The authentication process then proceeds according to the steps enumerated as follows:

Step (1) Remote client submits its user ID to the gateway inside https request.

Step (2) ~~In this step gateway~~ Gateway sends the counter's value (i) to the remote client along with the value of ~~secret~~ corresponding key (K_i).

The gateway ~~keeps~~ uses the counter (i) to index~~indexing~~ the number of successful user authentications. If N=100, the counter goes from 100 down to 1. When the counter reaches 0, no more authentications are allowed for a given user ID without re-initializing the key card.

Step (3) Client browser Plugin software decrypts the one time password (E_i) according to the expression: $[[S_i]]\underline{S_i}=D_{Ki\oplus Eks(PIN)}(E_i)$. Plugin sends S_i to the gateway's Key Card Authentication module.

Please replace Paragraph **[0052]** with the following paragraph rewritten in amendment format:

[0052] Communication between the remote client and the gateway begins with the remote client accessing a log-in page generated or served from pages stored in the template page database. This invokes the plug-in module, which then prompts the user to supply his or her log-in name or user ID. The user then enters his or her user ID, and this information is sent to the gateway where the ID is checked by the ASSM middleware and where the secure database is accessed to retrieve the values of $[[I]]\underline{i}$ and K_i that are appropriate for that user. Once these values are retrieved, the authentication process is ready to begin.

Please replace Paragraph **[0053]** with the following paragraph rewritten in amendment format:

[0053] The authentication process begins with the gateway communicating the index number i and the key value K_i to the remote client, which is operating using the plug-in module. In Figures 7 and 8 this first exchange of information (i, K_i) is illustrated at 200. The plug-in module uses the index value i to index into the table of one-time passwords, $E_1...\underline{E_N}[[E_i]]$. Note that these are encrypted passwords. In Figure 7 encrypted password E_i is retrieved by the plug-in module at 202.

Please replace Paragraph **[0055]** with the following paragraph rewritten in amendment format:

[0055] The plug-in module retrieves the encrypted session key K_s at 210 and then uses it at 208 to encrypt the user-supplied PIN. At this stage in the

process the plug-in module thus has the three pieces of information it needs to generate the one-time password, namely K_s, E_i and K_i.[[.]] The index value i is used to retrieve a selected one of the encrypted one-time passwords E_i at 202. The encrypted PIN E_{Ks}, is combined through an exclusive-OR (XOR) operation with the value K_i and the result is used ~~along~~ to decrypt the encrypted one-time password E_i. The decryption process is shown in Figure 7 at 214. The decryption process generates a single one-time password S_i, shown in Figure 7 at 216. This one-time password is then sent back to the gateway at 218. The gateway is then able to compare the one-time password with the stored one-time passwords within its secure database (secure database 73 of Fig. 4) to verify that the remote client is ~~or is not~~ authorized to proceed with secure communication.

Please replace Paragraph **[0059]** with the following paragraph rewritten in amendment format:

[0059] This reference then becomes the URL, which the remote client receives and subsequently would issue within its requests to the web proxy server. The overall process is shown in Fig. 10. When the modified URL arrives from the remote client to the gateway, the URL verification (validation) module 92 verifies its authenticity. The URL modification module then translates the URL into its regular form:

http://home_host/Original_URL

This then becomes the request that the web proxy issues over the trusted home network. Note that the URL modification process is bi-directional. Incoming URLs

from the remote client are modified specifically for that client (upon authentication). Similarly, outgoing URLs sent to the remote client are also modified using the same modification rules.

Please replace Paragraph **[0061]** with the following paragraph rewritten in amendment format:

[0061] The portable storage device by which one-time passwords are securely distributed to a remote client forms an important part of the network security system. As noted above, the system is designed to allow the user to conveniently configure his or her own portable storage device[[,]] using initialization and configuration software deployed at the gateway. The details by which the portable storage device[[s]] is configured will now be described in connection with Figure 11.

Please replace Paragraph **[0062]** with the following paragraph rewritten in amendment format:

[0062] Before the user can login from the remote location, he or she needs to initialize the portable storage device (remote key) by inserting it into ~~a slot of~~ the recording apparatus 36 on gateway 32. ~~In case the~~ If CD/DVD media is being used as [[a]] portable storage, the gateway 32 ~~device~~ must be equipped with a CD/DVD writer[[,]] capable of storing information into "user" and "protected" areas on the portable media. The process is shown in Fig. 11. The

remote key management module 70 (Fig. 4) performs the remote key initialization process.

Please replace Paragraph **[0064]** with the following paragraph rewritten in amendment format:

[0064] In step (3), the gateway's remote key management module obtains a User PIN from the authentication plug-in software at the user side, generates random K_s (step (4)), authenticates the key card, and stores K_s within the protected area of the portable storage device (step (5)).

Please replace Paragraph **[0065]** with the following paragraph rewritten in amendment format:

[0065] In step (6) the gateway's remote key management module 75 (Fig. 5) computes the value of $Ei = [[E_{ki}]]E_{Ki \oplus Eks(PIN)}(S_i)$ for each pair association (S_i, K_i). These values are then stored in the user data area of the portable storage device in step (7).

Please replace Paragraph **[0066]** with the following paragraph rewritten in amendment format:

[0066] Finally, the user's ID, user's PIN, K_s, and OTP key-password pairs (S_i, K_i) are stored in the secure database [[(]]73[[)]] (Fig. 4) for future reference by the Remote Key Authentication 70 and ASMM 72 modules (see Fig. 4). If any of

the above steps fails[[,]] for any reason, the overall portable storage device initialization process ~~must fail~~fails.